Guardian Digital
Secure Mail Suite

Quick Start Guide

Copyright © 2004 Guardian Digital, Inc.

Contents

1 Introduction **1**

2 Contacting Guardian Digital **2**

3 Purpose of This Document **3**

3.1 Terminology 3

3.2 Example Setup 5

4 Installing the Guardian Digital Secure Mail Suite **7**

4.1 Accessing the Installed Mail Suite 7

5 Adding Users **8**

6 General Configuration **10**

6.1 Setting Machine Hostname 10

6.2 Relay Host 11

6.3 Client Restrictions 11

7 Creating Virtual Domains **13**

7.1 Creating a virtual domain 13

7.2 Adding Users to a Virtual Domain 14

8 Create Mail Routes **16**

8.1 Creating A Mail Route 16

9 Message Filtering **18**

9.1 Enabling Virus Filter 18

9.2 Enabling Spam Filter 18

9.3 Enabling Outbound Scanning 19

9.4 Outbound Spam Protection 19

1 Introduction

Welcome to the Guardian Digital Secure Mail Suite!

Built on the foundation of EnGarde v1.5, the *Guardian Digital Secure Mail Suite* provides the ability to create a complete email system for an entire organization. Designed to meet the needs of small businesses, enterprise level companies, ISPs and ASPs looking to secure and manage corporate email operations, *Secure Mail Suite* is capable of managing all email functions within an organization.

Secure Mail Suite offers simplified administration capabilities to build a complete enterprise mail environment, and engineered to scale to thousands of users and domains. Through its use of advanced access control and authentication mechanisms, comprehensive auditing and reporting features, anti-spam and anti-virus protection, as well as encrypted communications facilities, *Secure Mail Suit*e delivers protection from constantly evolving online threats for both internal and external mail systems.

This manual is a quick introduction to help you set up *Secure Mail Suite*. For more detailed information about setting up and configuring the Guardian Digital *Secure Mail Suite*, Please refer to the complete *Secure Mail Suite* User Guide.

2 Contacting Guardian Digital

Guardian Digital welcomes your input and feedback. You may direct all questions, commands, or requests concerning the software you purchased, your registration status, or similar issues to the Guardian Digital Customer Service department at the following address:

Guardian Digital Customer Service
165 Chestnut Street
Allendale, New Jersey 07401
United States

Phone:	+1-201-934-9230
E-Mail:	customer.service@guardiandigital.com
World Wide Web:	http://www.guardiandigital.com
Online Store:	http://store.guardiandigital.com
Support:	support@guardiandigital.com

The department's hours of operation are 9:00 AM to 5:00 PM Eastern Time, Monday through Friday.

Guardian Digital provides comprehensive support for *Secure Mail Suite*. Refer to the *Secure Mail Suite User Guide* for more information about contacting Guardian Digital for support.

3 Purpose of This Document

This document is designed to give you a quick introduction for setting up a mail server using *Guardian Digital Secure Mail Suite*. This document covers basic configuration of *Secure Mail Suite*, along with providing step by step instructions for setting up a mail server. By the time you complete reading this guide, you should be able to

- *Create local user accounts*
- *Set a host name for your machine*
- *Set up a relay host.* Relay hosts are machines that will relay mail out to the Internet. Setting up a relay host for your mail server will cause it to send outgoing mail through the relay host.
- *Set client restrictions* Set up restrictions on senders for accepting mail.
- *Set up Virtual Domains and addresses* Set up the server as a mail store for a domain.
- *Create Mail Routes* Forward mail for specified domains to particular machines.
- *Set up Mail Filters* Setting up Spam and Virus Filtering on your mail server. Spam and Virus filtering components of Secure Mail Suite should be installed.

For more detailed instructions for configuring Secure Mail Suite, refer to the *Guardian Digital Secure Mail Suite User Guide.* You must refer to the corresponding manuals for configuring the *WebShare Manager* and *Mail List Manager* components of Secure Mail Suite.

3.1 Terminology

Simple Mail Transfer Protocol A protocol for sending e-mail messages between servers. Also commonly reffered as SMTP.

Fully Qualified Domain Name The full domain name that includes all higher level domain names.

Domain Name Service An Internet service that translates domain names into IP Addresses. Commonly referred to as DNS.

Spam Unwanted illegitimate bulk mail.

Mail Relay A server that routes an email to the correct destination. Mail relays are used to forward all mail for the local domain to the mail store.

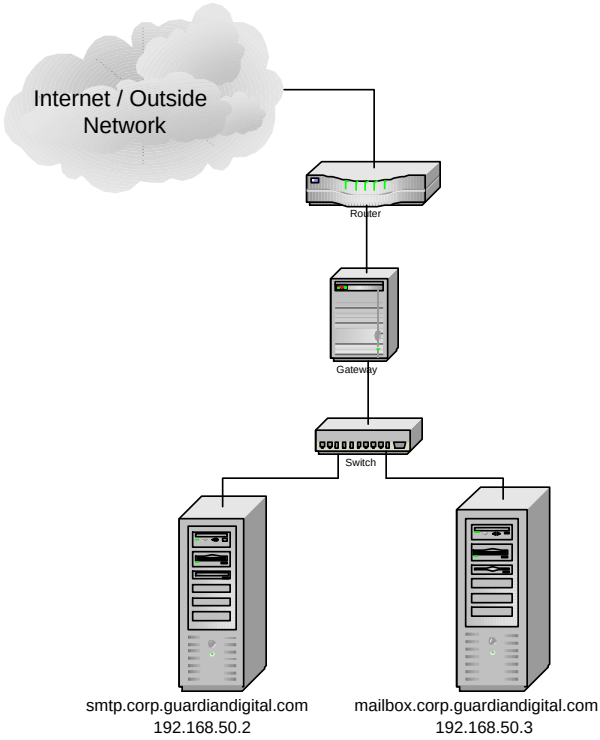
Domain A domain name is a name given to a group of machines. A domain name identifes one or more IP addresses. In an email address, the part to the right of '@' is the domain name.

Virtual Domain A domain that exists as a software entity on the server, which doesn't need a dedicated hardware location. A server can receive mail for a virtual domain.

3.2 Example Setup

The examples in this guide will use a real-life setup detailed below. The setup being used will have a main SMTP server which will act as a mail relay to a mailbox/spool server that stores the mail.

The following diagram outlines this configuration:



We will be using the 192.168.50.0/24 network (corp.guardiandigital.com) for our example. The two mail servers will be:

192.168.50.2 (smtp.corp.guardiandigital.com)
192.168.50.3 (mailbox.corp.guardiandigital.com)

Generally these two mail servers will be located on the same network, protected by a firewall. DNS service will be required. However, both the configuration of a firewall and DNS is beyond the scope of this guide.

Here, *smtp.corp.guardiandigital.com* is the SMTP server that receives mail from the Internet. *mailbox.corp.guardiandigital.com* is the mail store. *smtp.corp.guardiandigital.com* receives mail for the domain *corp.guardiandigital.com*, and forwards it to *mailbox.corp.guardiandigital.com*. *mailbox.corp.guardiandigital.com* stores mail for the domain *corp.guardiandigital.com*, and local users access it to read their mail. All local user accounts exist in *mailbox.corp.guardiandigital.com.*

You can create just one server to be a mail store without involving a relay. This means that the mail store must be able to receive mail directly from the Internet. Follow the instructions for creating a mailstore, but leave the *relay host* and *backup relay host* empty.

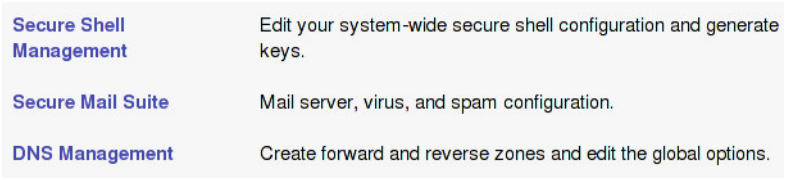
4 Installing the Guardian Digital Secure Mail Suite

Guardian Digital Secure Mail Suite is installed via the Guardian Digital Secure Network (GDSN). To install Secure Mail Suite insert the CD-ROM disk that was included with the Guardian Digital Secure Mail Suite purchase into the CD-ROM drive of the EnGarde server you will be installing the Secure Mail Suite on.

Selecting *Install from Local Media* in the GDSN will perform the installation. Instructions on how to use the GDSN can be found in *Section 5* on page *173* of EnGarde Secure Professional User Manual. Additionally, the *Install from Local Media* portion can be located on page *175* under *Section 5.1.2 Install from Local Media*.

4.1 Accessing the Installed Mail Suite

Once the GDSN finishes installing all of the Secure Mail Suite packages, the Secure Mail Suite portion will be accessible from the WebTool located in place of the original *Mail Configuration* option in the *System Management*, now labeled as *Secure Mail Suite*.

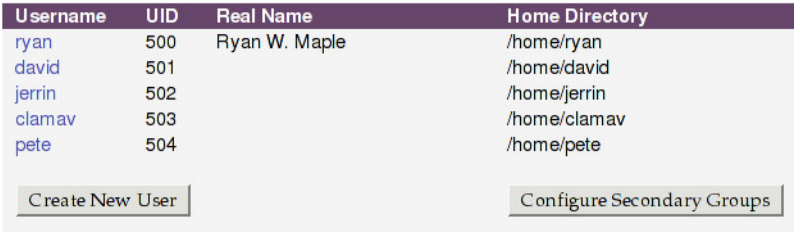

Secure Shell Management
Edit your system-wide secure shell configuration and generate keys.
Secure Mail Suite
Mail server, virus, and spam configuration.
DNS Management
Create forward and reverse zones and edit the global options.

5 Adding Users

After installing Secure Mail Suite, you must create local user accounts. You need to create user accounts only if this machine is a mail store. You must create a user for each mail account to be hosted here.

This section describes how to set up users for Secure Mail Suite. To add a user, go to the *System Management* section from the main index page. User creation and management is done in the subsection *Local User Management*.

To create a user, click *Create New User*.



The following options are provided for creating a user.

Username The username that we want to create

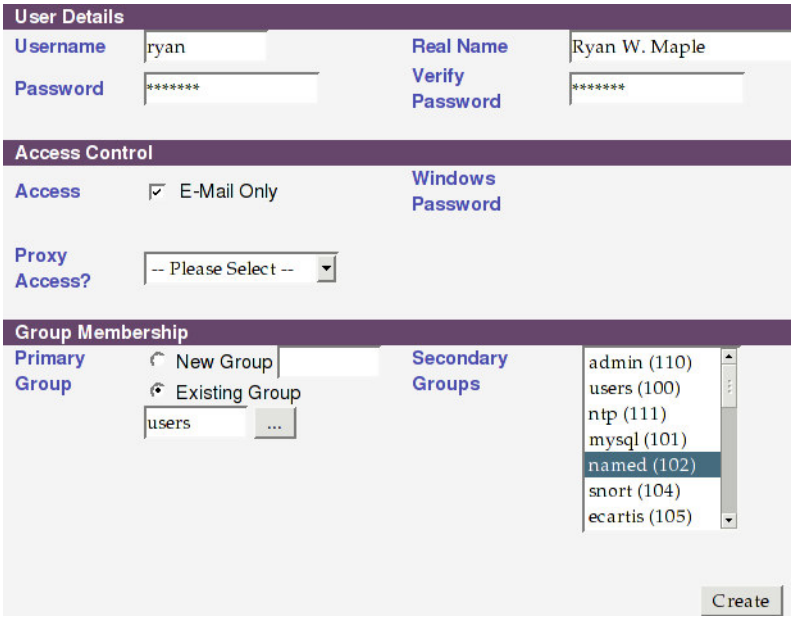
Real Name Full name of the person using this username.

Password The password of this user.

Verify Password Enter the password here also. This field is to verify that there are no spelling mistakes in the password.

Access Check *E-Mail Only* if this user account is for receiving email only. If checked, the user will not have shell access to the system.

Group Membership Each user should belong to a group. You can either create a new group for this user, or add this user to an existing group.
To create a new group, select *New Group* and enter the name of the group in the box. The group will be automatically created and the user will be added to that group.
To add the user to an existing group, select *Existing Group* and enter the name of the group on the box below. The user will be added to that group.



When all the necessary fields are completed, click *Create* to add the user. Once created, the user will be listed in the *Local User Management* section.

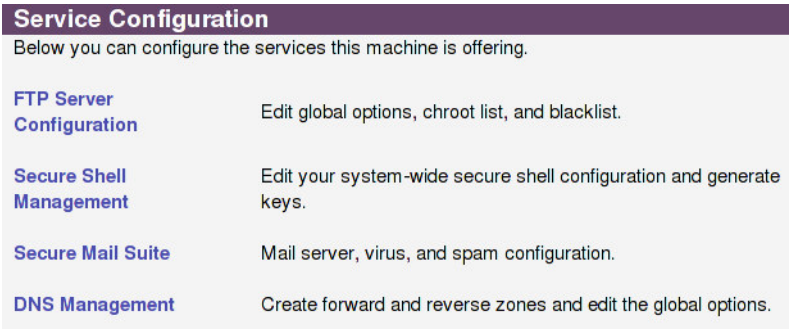
In the example configuration *mailbox.corp.guardiandigital.com* is the mail store. So we need to create local users in *mailbox.corp.guardiandigital.com.* Since *smtp.corp.guardiandigital.com* is a mail relay, there is no need to create local users on that machine.

6 General Configuration

This section outlines the basic steps needed to set up this machine as a mail server. The first step would be to give this machine a hostname. After that, you can specify a relay host, if needed. Relay hosts need to be created only if this machine cannot send mail directly to the Internet. If defined, the mail server will forward all outgoing mail to the relay host.

You should select a client restrictions policy for this mail server. These restrictions are applied to machines trying to send mail to our server. Client restrictions help reject illegitimate mail, mostly spam.

Accessing Secure Mail Suite To access the Secure Mail Suite from the WebTool, go to section *Main Index :: System Management* . Now click *Secure Mail Suite* under *Service Configuration* section. An index page will be displayed, from which you can easily access various components of the *Secure Mail Suite.*


Service Configuration
Below you can configure the services this machine is offering.
FTP Server Configuration
Edit global options, chroot list, and blacklist.
Secure Shell Management
Edit your system-wide secure shell configuration and generate keys.
Secure Mail Suite
Mail server, virus, and spam configuration.
DNS Management
Create forward and reverse zones and edit the global options.

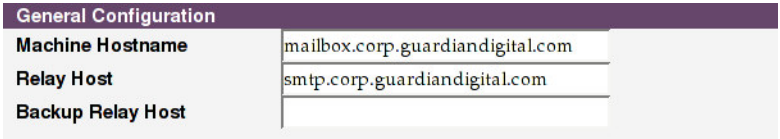
Go to *SMS :: General Configuration* by clicking *Server Configuration* in the section *General Configuration.*

General Configuration
Server Configuration
Setup basic mail server configuration.
Secure User Manager
Define what local users may use Secure User Manager features.

6.1 Setting Machine Hostname

You must give this machine a hostname before setting up the mail server. Enter the hostname in *Machine Hostname* option and click the *Save Configuration* button in

the bottom of the page. The hostname should be the fully qualified domain name (FQDN) of the machine. In the following example, we set the machine hostname as *mailbox.corp.guardiandigital.com.*



Also, you need to create an entry for the hostname and assign it to an MX record in your DNS server. Refer to the Engarde User Manual for instructions for doing this. You must be able to resolve the IP address of the machine using the hostname. In this example, the name mailbox.corp.guardiandigital.com should resolve to the IP address of this machine, using DNS.

6.2 Relay Host

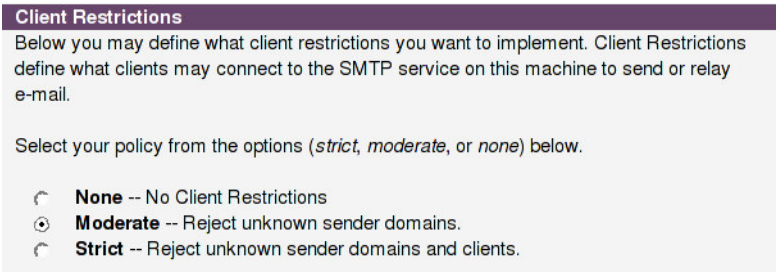
If the machine needs to pass mail to another mail server to get out to the Internet, the hostname of the mail server should be defined as the *Relay Host*. If a *Relay Host* is defined, mail to all domains not defined as a *mail route* or *virtual domain* will be forwarded to the machine defined as *Relay Host.* Generally, this option is used to relay outgoing mail.

In the above screen-shot example, the machine hostname is set as *mailbox.corp.guardiandigital.com* and it forwards all outgoing mail to the machine *smtp.corp.guardiandigital.com*. *smtp.corp.guardiandigital.com* sends the mail out to the Internet.

You can set the *Relay Host* and *Backup Relay Host* in the *General Configuration* section. The machine will forward mail to *Backup Relay Host* if the *Relay Host* is not available or doesn't accept mail. Note that *Relay Hosts* and *Backup Relay Hosts* should have corresponding DNS entries. You should be able to resolve them to the corresponding IP addresses.

6.3 Client Restrictions

Client restrictions define how the machine accepts mail. It defines what machines may connect to this server and send or relay mail using the SMTP service. The client restrictions section provides three policy levels: *none*, *moderate* and *strict*.


Client Restrictions
Below you may define what client restrictions you want to implement. Client Restrictions define what clients may connect to the SMTP service on this machine to send or relay e-mail.
Select your policy from the options (strict, moderate, or none) below.
None -- No Client Restrictions
Moderate -- Reject unknown sender domains.
Strict -- Reject unknown sender domains and clients.

None If set to *none*, no client restrictions will be implemented. All connecting mail servers will be able to send mail to this server if the destination is valid for this server. This option should almost never be chosen.

Moderate Selecting *Moderate* rejects mail if either the sender domain or the recipient domain is not a FQDN (Fully Qualified Domain Name) or cannot be resolved by DNS. It will also reject mail if the sender hostname is in invalid format. This is the recommended option.

Strict Selecting *Strict* will set the mail server to reject all incoming mail where the sender's hostname cannot be resolved by DNS, in addition to all other restrictions at the *moderate* level. This setting may reject valid mail under certain circumstances and must be used with caution.

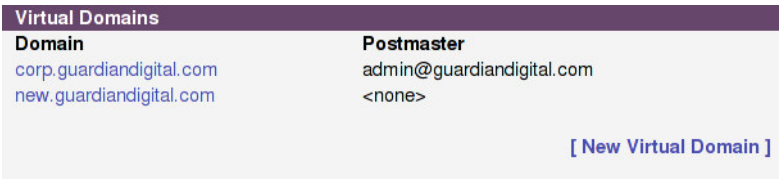
At this stage, you should have set up the mail server with user accounts, assigned it a hostname and optionally defined a relay host. At this point, the machine should be able to send mail out to the Internet. The following part of this guide will discuss how to configure this mail server to accept mail for a particular domain, or to forward mail for certain domains to other machines.

7 Creating Virtual Domains

You need to create *virtual domains* if this machine is to be a mail store. For example, if this machine is to accept mail for the email address *sales@corp.guardiandigital.com*, you must create a virtual domain *corp.guardiandigital.com* on this machine and add the user *sales* to that domain.

You don't need to create virtual domains if the machine only forwards or relays mail to other machines. Creating a virtual domain will make the machine the final destination for that domain.

You should have created an MX record for the virtual domain in your DNS server. The MX record should point to this machine. Refer to the Engarde User Manual for instructions about how to do this.



In the example setup, *mailbox.corp.guardiandigital.com* is the mail store for the domain *corp.guardiandigital.com*. So a virtual domain *corp.guardiandigital.com* should be created in *mailbox.corp.guardiandigital.com*.

7.1 Creating a virtual domain

Click *Virtual Domains* in the *Aliases, Domains and Routing* section. This page lists all virtual domains defined on this mail server. To create a new virtual domain, click *New Virtual Domain.* A pop-up window will come up with the following options.

Virtual Domain Enter the virtual domain here.

Postmaster The postmaster is an email address of a real user that will act as a default (sometimes called *catchall*) email address. If an email is sent to a user that doesn't exist in the virtual domain, the postmaster of that domain will receive the mail. This is an optional field. If the postmaster is not defined, mail to unknown users will be rejected.

Now click *Create Domain* to create the virtual domain.

In the example, the virtual domain *corp.guardiandigital.com* will be created, with postmaster *admin@guardiandigital.com*.

You should have configured DNS so that all mail for *corp.guardiandigital.com* reaches this machine. This is done by adding a MX record for the domain *corp.guardiandigital.com* in the DNS server, that points to this machine. If the MX record of *corp.guardiandigital.com* points to another machine (say *smtp.corp.guardiandigital.com*), you must configure that machine (*smtp.corp.guardiandigital.com*) to forward all mail in the domain *corp.guardiandigital.com* to this machine using a mail route.

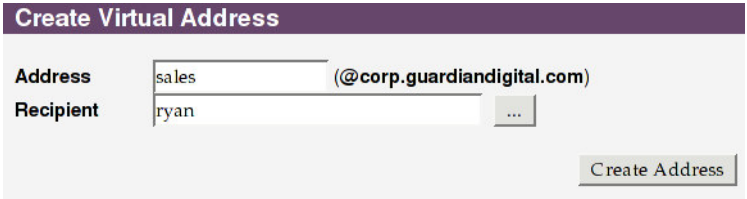
7.2 Adding Users to a Virtual Domain

After creating a virtual domain, you must create addresses in that domain. After you have created an address, the mail server will be able to receive mail for that address.

To create an address in a virtual domain, click the name of the domain. A pop-up window will come up listing all existing addresses in that domain.

To create a new virtual address, click *New Address.* Now enter the address and the recipient. The recipient can be a full email address to another destination or a local

username (one of the users created in section 5.1). Click *Create Address* to add this address to the *virtual domain*.



In the example we created an address *sales* in the virtual domain *corp.guardiandigital.com*, with the recipient as the user *ryan*. Now, the server will receive mail for *sales@corp.guardiandigital.com* and deliver them to the mailbox of local user *ryan*.

In the screen-shot example, two addresses are created in the virtual domain *corp.guardiandigital.com*: *sales@corp.guardiandigital.com* and *support@corp.guardiandigital.com*. All mail to these two addresses will be delivered to the accounts of local users *ryan* and *jerrin* respectively. Mail to any other address in the domain *corp.guardiandigital.com* (mail to say *ryan@corp.guardiandigital.com*) will be sent to the postmaster (*admin@guardiandigital.com*).

At this point, you should have set up at least one virtual domain in the machine configured as mail store, created addresses in it and set up a DNS server with an MX record pointing to the mail store. Now, you should be able to receive mail for the virtual domain.

8 Create Mail Routes

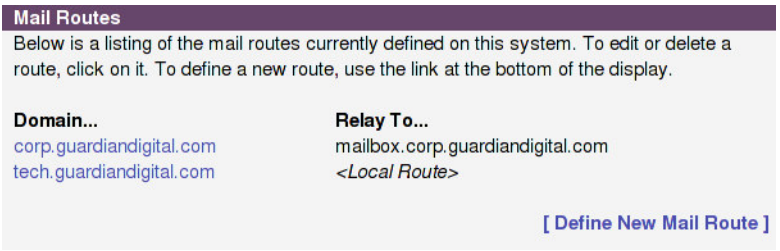
You need to create mail routes if this mail server is to relay mail to another machine. Mail routes are used to forward mail for a domain to the machine serving as mail store for that domain.

Each mail route has a domain name and a destination. A mail route tells the server to relay mail for a particular domain to a particular machine. You must create a mail route for every domain this server is to relay mail for.

In our example setup, the machine *smtp.corp.guardiandigital.com* should relay all mail for the domain *corp.guardiandigital.com* (Eg: mail to *sales@corp.guardiandigital.com*) to the machine *mailbox.corp.guardiandigital.com*. So, a *mail route* should be created in *smtp.corp.guardiandigital.com* that forwards mail for the domain *corp.guardiandigital.com* to the machine *mailbox.corp.guardiandigital.com.*

8.1 Creating A Mail Route

To create a mail route, go to section *Aliases and Routing.* All existing mail routes are listed in the section *Mail Routes* in the bottom of this page.


Mail Routes
Below is a listing of the mail routes currently defined on this system. To edit or delete a route, click on it. To define a new route, use the link at the bottom of the display.
Domain...
Relay To...
corp.guardiandigital.com
mailbox.corp.guardiandigital.com
tech.guardiandigital.com
<Local Route>
[Define New Mail Route]

Click *Define New Mail Route* to create a new mail route. A pop-up window will appear with the following options.

Domain The domain name for which the server should relay mail.

Relay To To relay mail to another server, select *Remote Machine* and enter the name of the remote machine below. To deliver all mail for this domain locally, select the option *Local route, store locally*.

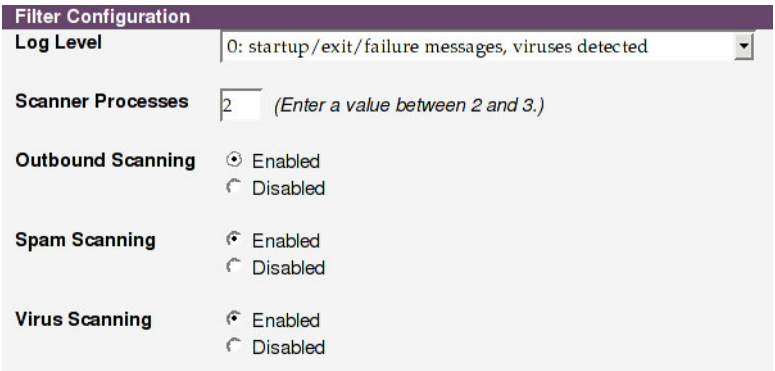
Click *Create Route* to create this mail route.

9 Message Filtering

Guardian Digital Secure Mail Suite provides protection against viruses and spam. By default, mail passing through the server is NOT scanned for viruses and spam. You can configure the mail filter extensively in *Content And Policy Enforcement (CAPE) Center :: Mail Filters.*

To perform basic filter configuration, go to the section *Content And Policy Enforcement (CAPE) Center :: Mail Filters :: General Filters.*

NOTE*:* This section only applies to those systems that have installed CAPE Center capabilities. Contact your local Guardian Digital sales representative for further information.



9.1 Enabling Virus Filter

Virus scanning can be enabled or disabled in the *Filter Configuration* section. To enable virus filtering, set the option *Virus Scanning* to *Enabled* and click *Save Configuration.*

9.2 Enabling Spam Filter

Spam scanning can also be enabled or disabled from the *Filter Configuration* section. To enable spam filtering, set the option *Spam Scanning* to *Enabled* and click *Save Configuration.*

9.3 Enabling Outbound Scanning

You may enable or disable scanning outbound mail in the *Filter Configuration* section. To enable scanning outgoing mail, set the option *Outbound Scanning* to *Enabled* and click *Save Configuration*. Now all mail going out to the Internet will be scanned for spam and viruses.

9.4 Outbound Spam Protection

If you enabled *Outbound Scanning* (described above), mail going out to the Internet will be scanned for both virus and spam. In many cases, scanning outgoing mail for spam may not be necessary if there is no probability of local users sending spam. Some of the legitimate outgoing mail may looks like spam, and they may be tagged as spam before getting sent to the recipient. This section describes how to exclude outgoing mail from being scanned for spam.

Go to *Content And Policy Enforcement (CAPE) Center :: Mail Filters :: Spam Filter Settings :: Outbound Spam Protection*. Here you can define whitelists for domains excluded from spam scanning.

For example, if your domain is *corp.guardiandigital.com*, you probably don't want mail from the domain *corp.guardiandigital.com* to be spam scanned. In this case, you need to create an *Outbound Domain Whitelist* entry for the domain *corp.guardiandigital.com*.

Outbound Domain Whitelist
[Edit] .corp.guardiandigital.com
[Edit] corp.guardiandigital.com
[New Outbound Whitelist Entry]

To create a new whitelist entry, click *New Outbound Whitelist Entry*. A pop-up window will come up. Enter the domain name in the field *Pattern*. You may choose to create an additional entry for all sub-domains.

Once created, the entry will be listed in the *Outbound Domain Whitelist*. In the example, all mail from *corp.guardiandigital.com* (Eg: mail from *admin@corp.guardiandigital.com*) will not be scanned for spam. The entry *.corp.guardiandigital.com* stands for all sub-domains of the domain *corp.guardiandigital.com*. (Eg: *hr.corp.guardiandigital.com*).